Information Security Policy

CyberAgency Group

CyberAgency Group is committed to protecting the confidentiality, integrity, and availability of the information we handle, whether it belongs to our clients, our partners, or our own business. This policy summarises the principles that guide how we manage information security across our organisation.

Our Commitment

- Protecting information from unauthorised access, disclosure, modification, or destruction.
- Managing information security risks through a systematic, documented, and evidence-based approach.
- Complying with all applicable legal, regulatory, and contractual obligations, including the Privacy Act 1988, the Notifiable Data Breaches scheme, and the Cyber Security Act 2024.
- Ensuring every team member understands and fulfils their information security responsibilities.
- Continually improving our security practices through regular review, audit, and corrective action.

How We Manage Security

Our information security management system (ISMS) is aligned with ISO/IEC 27001:2022. It is led by our senior management team and covers areas including:

- Risk assessment and treatment, to identify and manage information security risks.
- Access control, encryption, and information classification, proportionate to the sensitivity of information.
- Security awareness training for all personnel, refreshed on a regular basis.
- Backup, continuity, and incident response processes to protect the availability of critical systems.
- Regular internal audits and management reviews to drive continual improvement.

Scope

This policy applies to all CyberAgency Group employees, contractors, and authorised third parties who access, process, store, or transmit information on our behalf, across all the environments in which we operate.

Review

This policy is reviewed at least annually, and whenever a significant change, security incident, or audit finding warrants it, to ensure it remains current and effective.